CSC

The Intersection of Your Cybersecurity Posture with Domain Name Management

CSC insight paper

Contents

Cyber risk managed at the speed of AI

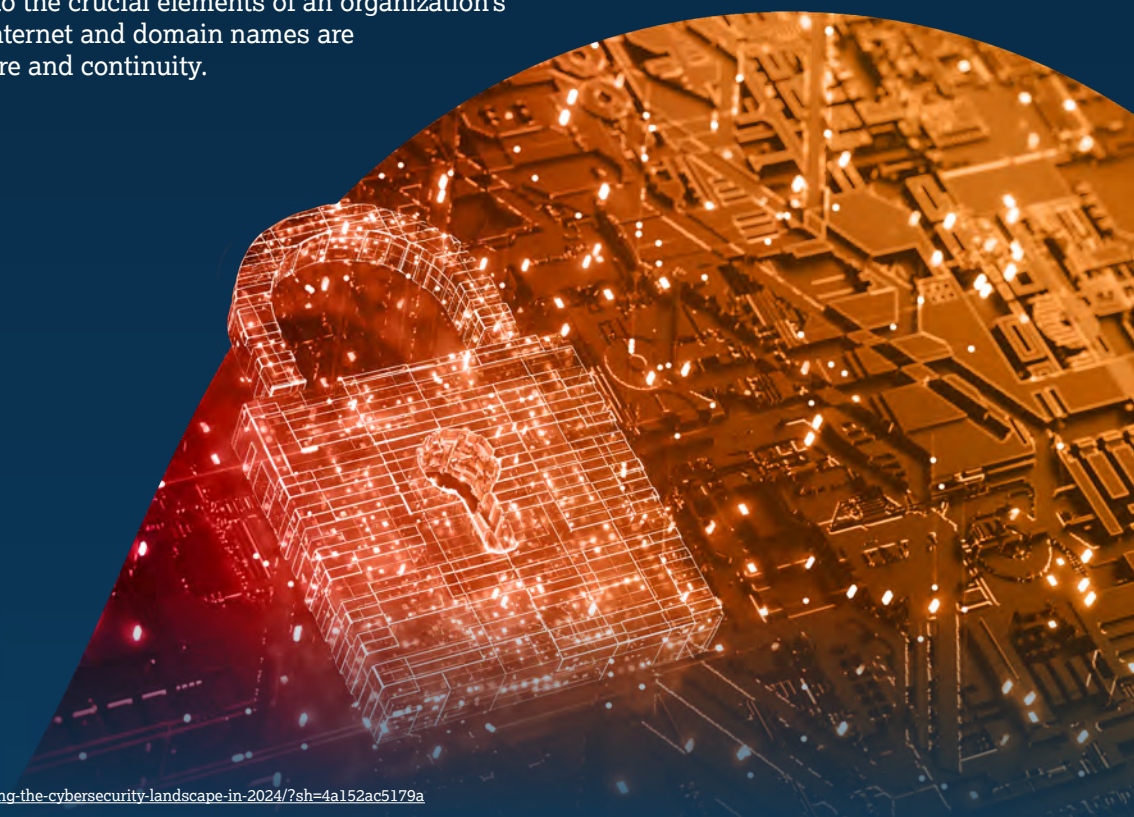
With the growth of artificial intelligence (AI) and the exponential increase in the complexity of cyber threats, companies and individuals alike need to significantly increase efforts in protecting against critical cyber risks. What's equipping bad actors with the potential to do more harm in less time is exactly what's also supporting better cyber defense strategies.[1] AI findings from a recent Splunk study[2] show that 70% of senior security executives believe AI gives advantages to attackers more than defenders, yet 35% are already experimenting with it for cyber defense.

Although, it's not all doom and gloom. A recent report by Goldman Sachs suggests that generative AI could raise gross domestic product (GDP) by 7%, a truly significant effect for any single technology. Yet cybercriminals are also using generative AI in targeted attacks to achieve higher sophistication and deployment speed. Generative AI is also enabling bad actors to craft personalized and targeted phishing emails that are free from spelling errors and have proper grammar—making such emails harder to detect. Currently available Dark Web AI tools—such as FraudGPT—enable bad actors to launch more complex, socially engineered deepfake attacks that manipulate the emotions or trust of targets even faster.

Domains are the foundation where cyber attacks are launched from

In a world where phishing attacks, business email compromise (BEC), and social engineering lead to even more complex attacks—such as malware and ransomware—it's surprising that chief information security officers (CISOs) don't pay more attention to their domain names and the external attack surface that exists online. They focus a lot of time on fortifying their network, but the perimeters have changed. Many CISOs are unaware who their domain registrars are, much less whether they provide the right enterprise level of security.

Global businesses rely on the internet for everything—websites, email, authentication, voice over IP (VoIP), client portals, supplier applications, and more. It's part of an organization's external attack surface and needs to be continuously monitored for cybercrime and fraud. As cyber risks continue to increase, organizations and cyber insurers face greater challenges in quantifying cyber risks and addressing their capacity for harm. This puts domain names right into the crucial elements of an organization's cybersecurity posture since the internet and domain names are essential to business infrastructure and continuity.



1. forbes.com/sites/emilsayegh/2023/12/19/navigating-the-cybersecurity-landscape-in-2024/?sh=4a152ac5179a
2. splunk.com/en_us/form/ciso-report.html

"Domain names, which run vital business functions, are in an ecosystem that, to any organization, should be considered part of the external attack surface. They live in an environment where domain names, along with subdomains, can be either compromised (hijacked) literally or maliciously registered, meaning brand lookalikes that are fake websites impersonate a brand for nefarious purposes, such as BEC attacks, or phishing and malware distribution attacks. One thing that many people are surprised about is the basic fact that anyone can register a domain name as long as it's available. So, if you don't acquire registrations for domains that use your brand or don't use homoglyphs and other strategies to look after your brand, there will always be fraudsters online trying to make money off your brand and its established trust. In turn, this puts both your revenue and reputation at risk, not to mention consumer safety concerns that come into play."

Ihab Shraim, chief technology officer,
CSC's Digital Brand Services in Safety Detectives interview

There are several ways organizations and their domains can be attacked:

Compromised domains or hijacked subdomains

Cyber criminals will compromise any domains left unsecured. Companies should start with a layered, defense-in-depth approach to protect against this. First and foremost, companies need to secure their brand's online presence by securing the domain portfolio—which may consist of multiple brands through acquisitions—and an online domain name system (DNS) footprint.

Creation of malicious, fraudulent domains

While some countries restrict who can register with their extensions by requiring a registered trademark, registered company, or local presence, one thing that can be alarming to learn is anyone can register any domain. The intent of these fake domain registrations is to leverage the consumer trust in the targeted brand to launch convincing phishing attacks, other forms of digital brand abuse, or intellectual property (IP) infringement. That leads to revenue loss, traffic diversion, and a diminished brand reputation for the organization in question—while putting money in the pockets of fraudsters. There are endless domain spoofing tactics using permutations and homoglyphs that are easily used by phishers and malicious third parties.

Newly lapsed brand domains re-registered by a third party

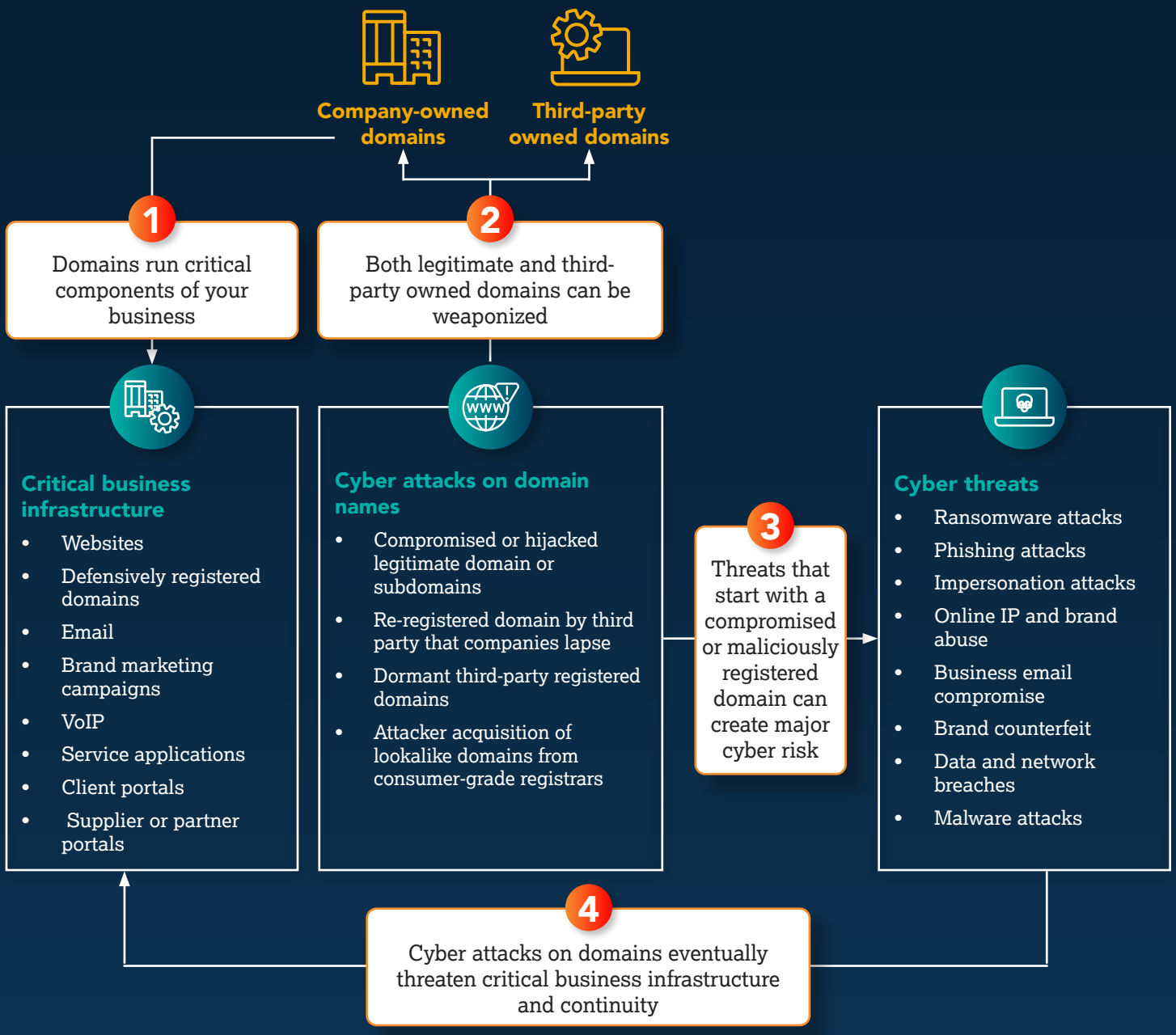
Companies defensively register critically important domain names to prevent online fraud for their brand. Sometimes after the registration, these organizations face cost pressures or the deceleration of a brand and let these domains lapse. Cybercriminals wait for this to happen and immediately re-register the same domain name for malicious purposes. They're constantly on the lookout for available, branded domains they can weaponize.

Dormant domains

Some cybercriminals may register and hold onto branded domains—perhaps hosting holding or parking pages, or displaying "site under construction" messaging—with the intent to resell them back to the targeted organization. They also may be plotting an even greater malicious activity such as a phishing or malware attack. A dormant domain name that's weaponized more than six months from its original registration date is a "submarine domain." Dormant domains often escape initial detection because they don't immediately have any of the characteristics of a domain registered to launch an attack—e.g., an active MX record—which would usually raise a red flag. This leaves plenty of room for cybercriminals to build more complex and personalized attack campaigns that have more devastating ramifications.

Aside from the age of the domain, it's also important to actively monitor how close the domain registrations are to previously identified threats and see if there's a registration pattern. Registration patterns aren't easy to spot in one place, but if your domain registrar provides AI and machine learning technology across its proprietary data and across various top-level domains (TLDs), patterns can be identified across IP addresses. It's also vital to watch for mimicking behaviors in your domain activity. What we mean by that is if your brand is registering a series of new domains for a new product or service, are third parties doing so as well?

External attack surface of a domain



Most cybersecurity risks are common knowledge to business leaders—such as how crucial it is to protect against data breaches, identity and vulnerability management, access controls, data protection, stolen credentials, and the need to stay vigilant when it comes to social engineering tactics. However, when it comes to day-to-day cybersecurity protection, it's evident many teams are unaware of who is responsible for their organization's domain security. Domain names are frequently used for marketing and brand initiatives, meaning security teams may feel protecting online domain names belongs to Marketing or Legal. If organizations are unfamiliar with who their domain registrars are, chances are they're unaware of the policies the registrars use and the security measures in place for branded, trademarked domains.

Unfortunately, adversaries are privy to the growth in businesses' online presence leading them to take a special interest in targeting corporate domain names left exposed. Without bolstering an organization's security posture, it will find itself in the eye of the perfect storm—navigating a path fraught with domain and DNS attacks, risking potential financial and reputation devastation. CSC's *Domain Security Report* recently analyzed the companies on the Forbes' Global 2000 list, and of those organizations, nearly three quarters have implemented less than 50% of all domain security measures. This insight, coupled with many organizations' general lack of knowledge of their domain registrars suggests domain security tends to be placed on the backburner—possibly in part due to a lack of internal ownership.

The value of working with an enterprise-class registrar

There are two general categories of domain registrars—consumer grade and enterprise class. Consumer-grade registrars make up more than 99% of all registrars in the world, and are geared towards domain services, websites, email for personal use, entrepreneurs, and start-ups in their beginning stages. Enterprise-class registrars specialize in working with corporations and brand owners that require advanced business capabilities, expertise, and support staff in relation to domain and DNS management as well as security, brand and fraud protection, data governance, and cybersecurity.

Consumer grade vs. enterprise class

Consumer-grade registrars

A consumer-grade registrar is geared for domain services, websites, and email for personal use, entrepreneurs, and small businesses that are just getting started.

Enterprise-class registrars

An enterprise-class registrar specializes in working with corporations and brand owners that require advanced business practices, capabilities, expertise, and support staff in relation to domain and domain name system (DNS) management, as well as security, brand and fraud protection, data governance, and cybersecurity.

Enterprise-class registrars are relentless on security

- ICANN and registry accredited
- Full accounting of all your domains, DNS, and digital certificate providers
- Written request mandate (never via phone)
- Data and General Data Protection Regulation (GDPR) compliant
- Registry transfer-lock policy

- ISO 27001 accredited data centers
- SOC 2® compliance
- Third-party penetration and vulnerability testing
- Regular security tests, including SQL injection and XSS

- Know Your Customer (KYC) identity verification
- Office of Foreign Assets Control (OFAC) screening
- Global 24x7x365 in-house support in local languages
- Regular cybersecurity staff training

Best practice is to use an enterprise-class provider that has invested in people, process, and technology integrated with security in mind. While anyone can say they offer services that meet the needs of today's global corporations, the onus is on companies to do their homework to understand the differences between third-party providers. Companies need to understand how their choice of provider fits into decisions made about their organization's overall security posture, along with compliance and risk concerns.

Seven steps an enterprise registrar should take to secure your domain portfolio

Like managing a digital certificate portfolio, managing domain names can be complex. By taking these steps, you'll take control of critical company assets and reduce the security threats against your brand.

1

Like managing digital certificates with a public key infrastructure (PKI), managing a global portfolio of domain names in one management system provides consistent processes as well as securing assets that your company relies on.

Centralization

2

Once all your domain assets are centralized, you can benefit from automation through a number of application programming interfaces (APIs)—similar to managing digital certificates. Domain portfolio APIs should include options such as:

- Domain portfolio reporting
- Domain availability checks for new registrations
- Domain registration with order template capability to complete registrations for a wide range of extensions
- Name server and WHOIS contact updates
- DNS record retrieval and modification for names
- URL forwarding management
- Reporting on 10 types of security-related events on your domains for auditing or security information and event management service providers (SIEM) integration
- Digital certificate management, including ordering, renewing, retrieving, reissuing, and revoking certificates; status checking is available for all ordering and updating actions

Automation

3

It saves time to use a provider that understands the various jurisdictions for each domain name and makes sure your data is kept up to date and within the rules of the country or region.

Compliance

4

It's very important to have your domain names and DNS integrated to make changes quickly and securely.

Integration

5

Every company is different and may need a different set up. This could mean you have a very decentralized use of domains or they're segmented by business units. Having a system that can be managed by a diverse group requires a level of accommodation so the right users access the right information. Additionally, companies need to navigate and understand complex data on their domain portfolio. Businesses need to access data quickly in a secure, dependable, and feature-rich environment, allowing for analysis of large volumes of information to make data-driven decisions. Reports that are necessary to review regularly include:

- **Live site status** – Visibility into whether a domain is resolving to content
- **Brand string counts** – Insights into how various brands are represented within the portfolio
- **Country** – Understanding how a brand's global presence is being used

Flexibility

6

Every year, more and more new domain names launch, and you need to make sure your business is making the right decisions on what to register based on potential threats. It's helpful to have a team of strategic advisors to support protecting your brand. They can help answer important questions such as:

- Do I have the right number of domains, or should I consider extending my defensive registrations to mitigate more risk?
- Is there an end-to-end workflow in place to mitigate domain-based attacks with threat intelligence?
- How do I know where to register a domain?
- What are the risks if I don't register?
- How do I communicate within my organization and register domains centrally?

Changing landscape

7

No company can register every variant domain name, so having an effective domain monitoring solution in place can spot when third parties are taking advantage of your brand name.

Monitoring

Work with an enterprise-class registrar to assess impact on your domains and DNS due to the European NIS2 Cybersecurity Directive

What it is:

"By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers."[3]

Why it's happening:

"The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. It modernized the existing legal framework to keep up with increased digitization and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole."[4]

3. nis-2-directive.com/NIS_2_Directive_Article_21.html#:~:text=By%2017%20October%202024%2C%20the,service%20providers%2C%20content%20delivery%20network
4. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

The risks of choosing a consumer-grade registrar

When companies are looking to cut back on costs, culling the domain portfolio can be viewed as an easy target. This short-term fix can lead to the long-term risk of domains being attacked by bad actors siphoning revenue away from the genuine brand, among other things.

Domain security should be an essential branch of cybersecurity to protect brands online, but it's not always the highest priority for consumer-grade domain registrars.[5] There's often misplaced trust put into consumer-grade registrars because they often weren't designed with domain security as a priority. That misplaced trust can impact a company's overall security posture.

Many companies have a misconception that all registrars are the same.

Consumer-grade domain registrars offer very transactional relationships with their clients, and don't go through the thorough review process an enterprise-class provider does. They don't offer solutions to mitigate all the digital risks of domain spoofing, domain and DNS hijacking attacks, sub-domain takeovers, and phishing attacks. Some consumer-grade registrars have business practices that may inadvertently harm brands. Some operate domain marketplaces that drop-catch, auction, and sell branded or trademarked domain names to the highest bidder, or undertake domain name spinning and advocate the registration of trademarked domains that proliferate typo-squatting. While these practices do not directly compromise businesses, they encourage brand abuse, or the registration of confusingly similar domain registrations that could be used for nefarious purposes.

We've all heard the term "you're only as strong as your weakest link." Every business relies on a series of suppliers and vendors, and with a complex series of vendors and workflows comes an increased risk for supply chain attacks. A supply chain attack is a cyber attack that occurs when a threat actor compromises a brand's system through a third-party partner with access to your systems and data. Typically, the vendor with the weakest cybersecurity posture is targeted.

An attack on your provider affects you too. The last two years have seen a few notable supply chain attacks. It's important to ensure the domain registrar for any business is secure and not at risk of being compromised. Domain registrars should be vetted by a team that fully understands the role a domain registrar plays in the company's overall security posture. It's important to monitor a vendor's breach record. Security-focused domain registrars can ultimately alleviate some of the burden from security teams and allow companies to catch threats in their domains before substantial damage to their brand is done.

"As described in its 10K filing for 2022, released Feb. 16, the company has been breached once every year since 2020 by the same set of cyber attackers, with the latest occurring just last December. It's worth also mentioning that the company has been the subject of earlier cyber incursions as well. The consequences to GoDaddy® are one thing, but, more notably, the breaches have led to data compromises for more than 1 million of the company's users."[6]

-- *Dark Reading,* "What GoDaddy's Years-Long Breach Means for Millions of Clients"

5. cpomagazine.com/cyber-security/the-glaring-gap-in-your-cybersecurity-posture-domain-security/
6. darkreading.com/cyber-risk/what-godaddy-years-long-breach-means-millions-clients

Mitigating the risk of compromised legitimate domains with a layered defense-in-depth strategy

To mitigate the risk of cyber attacks, the principles of defense in depth can be used for domain security. Defense in depth is an approach that started as a military strategy to protect a targeted asset. For domain security, it provides the coordinated use of multi-layered security countermeasures.

While anyone can say they offer services that meet the needs of today's global corporations, each company has to take the time to understand the differences between third-party providers. Businesses need to understand how their choice of provider fits into decisions made about their organization's overall security posture, along with concerns about IP infringement and trademark law.

1

Establish that your domain registrar is enterprise class

When it comes to the domain ecosystem, choice of domain registrar can impact colleagues responsible for cybersecurity and IT, legal (general counsel), and risk, and compliance (chief risk officer), as well as phishing attacks, online fraud, and brand abuse. To manage a company's domain name portfolio, you need to work with a provider that has invested in protecting its own systems.

2

Only work with a registrar that provides secure access to your domain management platform

The second layer in a defense-in-depth approach for domain security is to ensure your registrar mandates secure access to the domain and DNS management system. Registrars should require two-factor authentication for all their clients. They should also offer IP validation and federated ID so their clients can log into their network and know they have secure authentication into their domain management platform.

3

Be certain all user permissions are controlled and managed

When working with a registrar, it's crucial that it offers granular levels of permissions. The registrar should allow you access to manage user access and permissions. It should provide visibility on elevated permissions, including notifications when changes occur. This is especially important in the event of a cyber attack. If an attacker gets access to a registration system, they'll either create a new user or change the permissions on an existing user so they can do damage.

4

Use advanced domain security features

The fourth layer of the defense-in-depth approach is to apply advanced security features at the individual domain level. Once you have the pertinent domain names identified, it's time to apply the proper controls to it. First, there's registry lock—i.e., locking the domain name at the registry level—which disables automation between a registrar and a registry. This means the DNS can't be changed without a manual password that must be verified by an authorized contact to unlock the domain name. It's a highly secure, effective way to make sure that an important domain name's DNS can't be changed without the proper authorization.

How legitimate subdomains get hijacked without being hacked

Large organizations with diverse brand portfolios and international operations are often unaware of the scale of their globally dispersed, digital footprint. Digital records accumulate over time, and this makes cyber hygiene a real challenge. Businesses have been outsourcing to cloud providers for access to new technologies, yet the associated increase in DNS records—in addition to increasingly complex environments—opens them up to higher risk levels. Without proper oversight of digital records and daily monitoring, organizations accumulate "noise" that makes simple cyber hygiene more complex, resulting in easy exploits for cybercriminals.

"Digital records accumulate over time, and administrators who are unaware of each domain's history are hesitant to delete legacy records fearing they are tied to critical infrastructure. This buildup of inactive DNS zone records that do not point to content are known as "dangling DNS" and are at risk of subdomain hijacking where an attacker gains control of a legitimate subdomain that's no longer in use to host their own fraudulent or malicious content."

Mark Flegg, global director of security services in *SC Media*, "How to ensure DNS records don't become a security hazard"

Cybercriminals scan infrastructures such as the cloud and publicly available services. This includes searching DNS zone records that point to web services that are no longer used by a brand. By hosting content with cloud providers who don't run verification checks, criminals can request a previously used zone destination and start to receive web users landing on these subdomains—all loaded with their own illegitimate content—without infiltrating an organization's infrastructure or third-party service account. For example, it was reported by ZDNet that a global computing company was hijacked by bad actors to showcase poker casinos on their subdomains.

Taking advantage of dangling DNS records opens a gateway for other cyber attacks, such as phishing and malware distribution, which can result in revenue loss, data exfiltration, loss in consumer confidence, and reputation damage due to security breaches. Research conducted by Austrian IT security consulting firm Certitude Consulting was recently published in *Security Week* warning thousands of entities are vulnerable to such attacks. It's imperative that DNS records management needs to be part of today's cyber hygiene practices. For more than 20 years, companies have been at risk of mismanagement because they employ different owners, policies, and vendors to manage their DNS, which is further complicated if they undergo mergers and acquisitions, where there's also the inherent fear of deleting anything that owners are unsure about.

CSC's *Subdomain Hijacking Vulnerabilities Report* reviewed over 440,000 DNS records and found that over 21% of DNS records point to content that does not resolve, leaving many companies vulnerable to subdomain hijacking. Additionally, over 277,000 (63%) show error status codes such as "404 not found" or "502 bad gateway." DNS records housekeeping is historically one of the most frequently neglected tasks due to a long history of different owners, policies, and vendors. Digital records accumulate over time, and administrators who may be unaware of each domain's history are hesitant to delete legacy records fearing they may be tied to critical infrastructure. Dangling DNS are at risk of subdomain hijacking. Subdomain hijacking is where an attacker gains control of a legitimate subdomain that is no longer in use to host their own fraudulent or malicious content. This opens a gateway for other cyberattacks such as phishing, malware, and ransomware.

21%

of DNS active subdomain records do not resolve, leaving companies vulnerable to subdomain hijacking.

Online brand protection is a cybersecurity necessity

Maliciously registered domain names are often the precursor to full-blown targeted phishing or BEC campaigns that can be equipped with lethal downloadable malware. To prevent these initial exploitations, organizations need to assess the state of their domain landscape and remove the disconnect among teams responsible for handling this aspect of digital brand initiatives. Security teams must actively monitor their domains and brands online to reduce the potential of web domains using their brand name—or a version of it—for fraudulent activity.

Securing your domains is the starting point to stop phishing in its tracks.

Companies need better insight into bad actors who may be registering or re-registering lookalike domains attempting to pose as their online brand. This insight can help companies catch security incidents as they occur and enforce against them.

Historically, many companies don't understand the depth of the challenges and the growth in the number of channels where infringing activity takes place online. Companies invest time and money into building trusted brands, yet it could all mean nothing if they fall victim to online crime. The best way for companies to protect their brand is to implement an online brand protection program that combines online monitoring and enforcement activities to remove fraudulent content. Complementary solutions, like the use of blocking networks—that can incorporate partnerships with browser providers, internet service providers (ISPs) and other SIEMs—to block fraudulent websites from internet users, can also help create a more comprehensive approach. Using these methods to track and remediate activity by infringers should also run alongside a program of secure domain name management, allowing the brand owner to administer and protect their own official domain portfolio.

Revolutionizing the way you lower your cyber risk exposure online

As the leading enterprise-class domain registrar for the largest brands in the world, CSC is revolutionizing the domain name ecosystem. At CSC, we believe domain security intelligence is power.

DomainSec platform

DomainSec℠ is the industry's first holistic approach to securing and defending brands' domain ecosystems. It's the most innovative corporate domain management and security solution in the market, coupled with next generation online brand and fraud protection. Combining the data from these solutions together into one platform means CSC can offer exponentially better cybersecurity protection to bolster the corporate security posture. We can help brands refine their zero-trust security model, going beyond just safeguarding perimeters. This first-of-its-kind platform uses proprietary technology—combining machine learning, artificial intelligence, and clustering technology—to enable the smartest security insights using leading indicators.

View CSC's list of defensive and proactive security measures to safeguard your domains and brands using a multi-layered, defense-in-depth approach to domain security.

Download our *Domain Security Checklist.*

ABOUT CSC

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSec℠ platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia- Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve. Visit cscdbs.com.

Get in touch

cscdbs.com